

CLAIMS

We I claim:

1. A method for secure routing of information and addressing of a service and of parties to the service in a telecommunication system that includes a telecommunication terminal, a telecommunication network, a service provider connected to the telecommunication network, a service apparatus connected to the telecommunication network for mediating the service, and a communication link connecting the telecommunication terminal and the service apparatus, said method comprising the steps of:

providing the telecommunication terminal with a terminal-specific unambiguous identifier;

addressing the service apparatus from the telecommunication terminal by sending a predetermined connection setup request from the telecommunication terminal to the service apparatus;

providing at least one of the service apparatus and the service mediated by the service apparatus with a service-specific unambiguous identifier associated with predetermined keys for at least one of encryption and digital signing; and

sending one of a network address of the service provider and information relating to the mediated service from the telecommunication terminal to the service apparatus via the communication link.

2. A method in accordance with claim 1, wherein the service apparatus is addressed from the telecommunication terminal by sending the predetermined connection setup request from the telecommunication terminal to the service apparatus via the communication link.

5

3. A method in accordance with claim 1, further comprising the step of one of encrypting and digitally signing information sent from the telecommunication terminal using the keys associated with the service-specific unambiguous identifier, and wherein said sending step comprises sending the one of encrypted and digitally signed information from the telecommunication terminal to the service provider using an address determined by the telecommunication terminal.

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

4. A method in accordance with claim 1, wherein the service apparatus is controlled based on information sent by the service provider.

15

5. A method in accordance with claim 1, further comprising the step of sending, from the service provider to one of the service apparatus and the telecommunication terminal, a confirmation message.

20

6. A method in accordance with claim 1, further comprising the step of sending, from the service provider to one of the service apparatus and the telecommunication

terminal, a confirmation message confirming a service transaction if a predetermined condition has been fulfilled.

7. A method in accordance with claim 1, further comprising the step of
5 sending, from the service provider to one of the service apparatus and the telecommunication terminal, an SMS message confirming a service transaction.

8. A method in accordance with claim 1, wherein a service request from the telecommunication terminal is accepted only after the service apparatus has received from the service provider a confirmation code for a requested service transaction.

9. A method in accordance with claim 1, wherein the communication link comprises a Bluetooth communication connection.

10. A method in accordance with claim 1, wherein the communication link comprises an infrared communication connection.

11. A method in accordance with claim 1, wherein the communication link is encrypted.

12.. A method in accordance with claim 1, further comprising the step of using a public-private key encryption system for one of encrypting and digitally signing information exchanged between at least two of the telecommunication terminal, the service apparatus and the service provider.

5

13. A method in accordance with claim 1, wherein WAP is used in communications between the telecommunication terminal and one of the service apparatus and the service provider.

14. A method in accordance with claim 1, wherein the service provider communicates with a trusted third party that maintains a database containing one of encryption and digital signing keys associated with the unambiguous identifiers.

15. A method in accordance with claim 1, further comprising the step of sending a request, from one of the service provider and the service apparatus to a trusted third party that maintains a database containing one of encryption and digital signing keys associated with the unambiguous identifiers, a request for the keys.

16. A method in accordance with claim 1, wherein the network address is an IP address.

20

17. In a telecommunication system that includes a telecommunication terminal, a telecommunication network, a service provider connected to the telecommunication network, a service apparatus connected to the telecommunication network for mediating a service, and a communication link connecting the telecommunication terminal and the service apparatus, the improvement comprising a system for secure routing of information and addressing of the service and of parties to the service, said system comprising:

means for providing the telecommunication terminal with a terminal-specific unambiguous identifier;

means for addressing the service apparatus from the telecommunication terminal by sending a predetermined connection setup string from the telecommunication terminal to the service apparatus;

means for providing at least one of the service apparatus and the service mediated by the service apparatus with a service-specific unambiguous identifier associated with predetermined keys for at least one of encryption and digital signing; and

means for sending one of a network address of the service provider and information relating to the mediated service from the telecommunication terminal to the service apparatus via the communication link.

18. The system of claim 17, further comprising means for addressing the service apparatus from the telecommunication terminal by sending the predetermined

connection setup request from the telecommunication terminal to the service apparatus via the communication link.

19. The service of claim 17, further comprising:

5 means for at least one of encrypting a digitally signing information sent from the telecommunication terminal using the keys associated with the service-specific unambiguous identifier; and

10 means for sending the at least one of encrypted and digitally signed information over the telecommunication network to a network address determined by one of the telecommunication terminal and the service apparatus.

20. The system of claim 17, further comprising means for controlling the service apparatus based on information sent by the service provider.

15 21. The system of claim 17, further comprising means for sending, from the service provider to one of the service apparatus and the telecommunication terminal, a confirmation message.

20 22. The system of claim 17, further comprising means for sending, from the service provider to one of the service apparatus and the telecommunication terminal, a

confirmation message confirming a service transaction if a predetermined condition has been fulfilled.

23. The system of claim 17, further comprising means for only accepting a
5 service request from the telecommunication terminal after the service apparatus has received from the service provider a confirmation code for a requested service transaction.

24. The system of claim 17, further comprising means for encrypting the communication link.

25. The system of claim 17, further comprising a trusted third party that communicates with one of the service apparatus and the service provider over the telecommunication network.

15 26. The system of claim 17, wherein one of the service provider and the service apparatus comprises means for sending to a trusted third party a request for the one of the encryption and digital signing keys associated with the unambiguous identifier.

20 27. The system of claim 17, wherein the telecommunication terminal comprises a mobile station having a connected subscriber identity module.

28. The system of claim 17, wherein the service apparatus comprises an automated teller machine.

29. The system of claim 17, wherein the service apparatus comprises a cash
5 register system.

30. The system of claim 17, wherein the service apparatus comprises a computer.

31. The system of claim 17, wherein the service apparatus comprises an
10 automated service machine.

32. The system of claim 17, wherein the telecommunication network
comprises the Internet.

33. The system of claim 17, wherein the telecommunication network
15 comprises a bank payment network.